

MEL:RAS/JKW
F: #2021R00415

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
FACEBOOK USER ID 100001797777653
THAT IS STORED AT PREMISES
CONTROLLED BY FACEBOOK INC.

Case No. 21-MJ-1208

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, BRIAN G. GANDER, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with Facebook user ID 100001797777653 (the “Subject Account”) that is stored at premises owned, maintained, controlled, or operated by Facebook Inc. (“Facebook”), a social networking company headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the user ID.

2. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) and have been since approximately September 2002. As such, I am a “federal law enforcement officer” within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I am part of the Child Exploitation and Human Trafficking Task Force

with the FBI and New York City Police Department (the “Task Force”). I have extensive experience investigating cases relating to sex trafficking and sex trafficking of minors. I have experience executing search warrants on electronically stored communications of the sort requested herein.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 1591 (sex trafficking of a minor or by force, fraud, or coercion), 1594 (conspiracy to commit sex trafficking), 2251 (sexual exploitation of a minor), 2252 (child pornography offenses),¹ 2421 (the Mann Act) and 2422 (coercion and enticement) (the “Subject Offenses”) have been committed by ELIJAH WUSU, also known as “Lucky,” and others known and unknown. There is also probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

PROBABLE CAUSE

I. Background

5. Since at least February 2020, the Task Force has been investigating ELIJAH WUSU, also known as “Lucky,” for the Subject Offenses. As part of its investigation, the Task

¹ The terms “minor,” “sexually explicit conduct,” “visual depiction” and “child pornography” are defined as set forth in Title 18, United States Code, Section 2256.

Force has, inter alia, reviewed online advertisements for commercial sex, interviewed victims and obtained information from Internet and communications providers.

6. At least three victims, Victim-1, Victim-2 and Victim-3, reported to law enforcement that they engaged in commercial sex acts at the direction of WUSU, who used the name Lucky. Victim-3 was a minor at the time and Victim-1 and Victim-2 described either experiencing or witnessing violence or threats of violence by WUSU.

7. Further, as described in greater detail below, there is probable cause to believe that WUSU, using the Subject Account, attempted to recruit another minor, Victim-4, to engage in commercial sex acts on his behalf, although she did not ultimately work for him.

II. The Subject Account

8. On or about August 9, 2021, the Honorable Sanket J. Bulsara signed a warrant authorizing the search of an account, which at times used the vanity name “Vida Kashh” (the “Vida Kashh Account”). (21-MJ-935). Evidence obtained pursuant to the warrant showed numerous communications between the user of the Vida Kashh Account and other Facebook accounts, in which the user of the Vida Kashh Account referred to Luciano Gallucio – the username associated with the Subject Account – as her “daddy,” and directed others to contact Luciano Gallucio through the Subject Account.

9. Based on my training and experience, as well as my participation in this investigation, I understand the term “daddy” to refer to a male individual who directs the person or persons who refer to him as daddy to engage in commercial sex work. I further understand that the user of the Vida Kashh Account was directing women to the Subject Account for them to engage in commercial sex work at the direction of the user of the Subject Account.

10. Evidence obtained from the search of the Vida Kashh Account shows that the Vida Kashh Account was used to recruit Victim-1 and Victim-2, among others, to work for WUSU. Records show that between March 2019 and September 2019, Victim-1 communicated with the Vida Kashh Account, and in or about January 2020, Victim-2 communicated with the Vida Kashh Account. During these communications, the user of the Vida Kashh Account attempted to recruit each of the victims. For example, the user of the Vida Kashh Account told Victim-1 that she did “dates” and had a “daddy.” The user asked Victim-1 to “become part of the Team” and directed Victim-1 to call “Lucky.” The user of the Vida Kashh Account also asked Victim-2 if she was “about the stripping & trapping life.” The user of the Vida Kashh Account then told Victim-2 that Victim-2 needed to “come trap with [the] team,” saying she needed “some new trap sisters” and directing Victim-2 to call her “daddy . . . for an interview.”

11. Based on my training and experience, as well as my participation in this investigation, I understand the term “date” to refer to a meeting for the purpose of engaging in commercial sex; I understand the term “trap” or “trapping” to refer to engaging in commercial sex; and I understand the term “bag” to refer to money.

12. Evidence obtained from the search of the Vida Kashh Account shows communications in the Vida Kashh Account related to Luciano Gallucio between February 2019 and June 2021. For example, on or about February 15, 2019, the user of the Vida Kashh Account told another Facebook user (“Individual-1”) that she could get “paid for [her] time on a date.” The user of the Vida Kashh Account provided Individual-1 the name Luciano Gallucio after informing Individual-1 that she should call him “daddy” and that they do not “call him a pimp.” The user of the Vida Kashh Account then added the Subject Account (Luciano Gallucio) to the conversation and wrote, “Here [is] my friend she about a bag.” Based on my training and

experience, as well as my participation in this investigation, I understand the foregoing conversation to reflect the user of the Vida Kashh Account referring Individual-1 to the Subject Account to engage in commercial sex at the direction of the user of the Subject Account.

13. On or about and between July 25, 2019 and October 21, 2019, the user of the Vida Kashh Account communicated with another Facebook user (“Individual-2”). The user of the Vida Kashh Account advised Individual-2 that she was “Trappin.” The user of the Vida Kashh Account then told Individual-2 that she was “Tryin Come get a bag with the team,” that she could “hook” Individual-2 up with her “daddy” and that her “daddy” was Luciano Gallucio. After receiving the name Luciano Gallucio, Individual-2 advised that she was unable to find his account, at which time the user of the Vida Kashh Account clarified that Individual-2 could find him on “fb” or Facebook. Based on my training and experience, as well as my participation in this investigation, I understand the phrase “get a bag” to refer to making money and I understand the foregoing conversation to reflect the user of the Vida Kashh Account referring Individual-2 to the Subject Account to engage in commercial sex at the direction of the user of the Subject Account.

14. In another conversation on or about June 21, 2021, the user of the Vida Kashh Account told another Facebook user (“Individual-3”) that her “daddy” is named “lucky” and that his “ol fb [is] Luciano gallucio.” The user of the Vida Kashh Account then provided Individual-3 with a phone number for her “folks” as “1347-372-1561” (the “1561 Number”). The 1561 Number has been identified as being used by WUSU. Specifically, Victim-1 and Victim-2 used the 1561 Number to communicate with WUSU.

15. Based on the foregoing, there is probable cause to believe that the Subject Account was used in connection with sex trafficking and related offenses and that the Subject Account contains evidence of the Subject Offenses.

III. Victim-4 and the Luciano Gallucio Account

16. There is probable cause to believe the Subject Account was used to attempt to recruit Victim-4, a minor at the time, to engage in commercial sex work and to receive child pornography.

17. Victim-4 voluntarily provided law enforcement communications between a Facebook account that she identified as belonging to and being used by her (“Victim-4’s Account”) and a Facebook account with username “Luciano Gallucio” (the “Luciano Gallucio Account”).

18. At the time law enforcement obtained the communications from Victim-4, the Luciano Gallucio Account had been deactivated. However, there is probable cause to believe that the Luciano Gallucio Account is the Subject Account because the account names – Luciano Gallucio – are identical, and the user of the Luciano Gallucio Account identified himself in his communications with Victim-4 as “lucy,” which I understand to be an alternate spelling of “Lucky,” which is an alias WUSU uses.

19. Victim-4 used Victim-4’s Account to communicate with the Luciano Gallucio Account in September and October 2018, when Victim-4 was a minor. The Luciano Gallucio Account initiated the conversation and asked Victim-4, “U about getting cash”?

20. At the outset of the communications, Victim-4 repeatedly stated that she was seventeen years’ old.

21. Through September and October 2018, the user of the Luciano Gallucio Account repeatedly asked Victim-4 to engage in commercial sex work, and Victim-4 repeatedly declined. For example, on or about October 13, 2018, the user of the Luciano Gallucio Account stated in writing and audio messages, “U gonna be a paid bitch” and “we gonna get some money with that kitty you hear me? We gonna break them tricks you hear me?” Victim-4 responded, “I already told you . . . you’re not pimping me.” She further stated, “BOY I’M NOT SELLING PUSSY FOR YOU TF.” Based on my training and experience, as well as my participation in this investigation, I understand the term “tricks” to refer to a customer who pays another individual to engage in a sex act; I understand the term “kitty” to refer to the victim’s vagina; and I understand the foregoing statements to reference Victim-4 engaging in sex for money.

22. On or about October 14, 2018, the user of the Luciano Gallucio Account sent an audio message to Victim-4’s Account that stated, “this thing right here, this is a producible thing. When you with me it’s diamonds and furs and cars and houses.” Based on my training and experience, as well as my participation in this investigation, I understand the user of the Luciano Gallucio Account to be promising to provide valuable goods to Victim-4 if she engaged in commercial sex work for him.

23. Victim-4 also reported to law enforcement that she sent nude photographs of herself to the Luciano Gallucio Account when she was a minor.

IV. Facebook Generally

24. Facebook owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news,

photographs, videos, and other information with other Facebook users, and sometimes with the general public.

25. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

26. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

27. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

28. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post “status” updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming “events,” such as social occasions, by listing the event’s time, location, host, and guest list. In addition, Facebook users can “check in” to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user’s profile page also includes a “Wall,” which is a space where the user and his or her “Friends” can post messages, attachments, and links that will typically be visible to anyone who can view the user’s profile.

29. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to “tag” (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook’s purposes, the photos and videos associated with a user’s account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

30. Facebook users can exchange private messages on Facebook with other users. Those messages are stored by Facebook unless deleted by the user. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a chat feature that allows users to send and receive instant messages through Facebook Messenger. These chat communications are stored in the chat history for the account. Facebook also has

Video and Voice Calling features, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

31. If a Facebook user does not want to interact with another user on Facebook, the first user can “block” the second user from seeing his or her account.

32. Facebook has a “like” feature that allows users to give positive feedback or connect to particular pages. Facebook users can “like” Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become “fans” of particular Facebook pages.

33. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

34. Each Facebook account has an activity log, which is a list of the user’s posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as “liking” a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user’s Facebook page.

35. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

36. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications (“apps”) on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user’s access or use of that application may appear on the user’s profile page.

37. Facebook also retains Internet Protocol (“IP”) logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP

address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

38. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

39. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook

account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to “tag” their location in posts and Facebook “friends” to locate each other. This geographic and timeline information may tend to either inculcate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner’s state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

40. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

41. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Facebook to disclose to the government copies of the records and other information

(including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

42. Based on the foregoing, I request that the Court issue the proposed search warrant.

43. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Facebook. Because the warrant will be served on Facebook, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

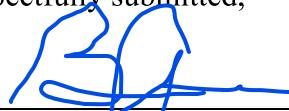
44. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

45. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING

46. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,



Brian G. Gander
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me by telephone
on October 25, 2021



HONORABLE CHERYL L. POLLAK
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Facebook user ID 100001797777653 that is stored at premises owned, maintained, controlled, or operated by Facebook Inc., a company headquartered in Menlo Park, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Facebook

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook Inc. (“Facebook”), regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for the user ID listed in Attachment A:

- (a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers;
- (b) All activity logs for the account and all other documents showing the user’s posts and other Facebook activities;
- (c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them, including Exchangeable Image File (“EXIF”) data and any other metadata associated with those photos and videos;
- (d) All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends’ Facebook user identification numbers; groups and networks of which the user is a member, including the groups’ Facebook group identification

numbers; future and past event postings; rejected “Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Facebook applications;

- (e) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;
- (f) All other records and contents of communications and messages made or received by the user from September 1, 2018 to present, including all Messenger activity, private messages, chat history, video and voice calling history, and pending “Friend” requests;
- (g) All “check ins” and other location information;
- (h) All IP logs, including all records of the IP addresses that logged into the account;
- (i) All records of the account’s usage of the “Like” feature, including all Facebook posts and all non-Facebook webpages and content that the user has “liked”;
- (j) All information about the Facebook pages that the account is or was a “fan” of;
- (k) All past and present lists of friends created by the account;
- (l) All records of Facebook searches performed by the account from September 1, 2018 to present;
- (m) All information about the user’s access and use of Facebook Marketplace;
- (n) The types of service utilized by the user;

- (o) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- (p) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account; and
- (q) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

Facebook is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 1591 (sex trafficking of a minor or by force, fraud, or coercion), 1594 (conspiracy to commit sex trafficking), 2251 (sexual exploitation of a minor), 2252 (child pornography offenses), 2421 (the Mann Act) and 2422 (coercion and enticement) (the “Subject Offenses”) involving ELIJAH WUSU, also known as “Lucky,” and others known and unknown since September 1, 2018, including, for each user ID identified on Attachment A, information pertaining to the following matters:

- (a) Communications, records, or activity relating to commercial sex;
- (b) Communications, records, or activity concerning the recruitment or grooming of victims (both identified and unidentified) of the Subject Offenses;
- (c) Communications, records, or activity regarding the planning, execution, and cover up of the Subject Offenses;
- (d) Communications with co-conspirators regarding the Subject Offenses;
- (e) Communications, records, or activity concerning ELIJAH WUSU, also known as “Lucky,” and any of his co-conspirators;
- (f) Photographs, videos, images, audio, and other content relating to victims (both identified and unidentified) of the Subject Offenses;
- (g) Communications with individuals about sexual acts involving minors, including but not limited to communications relating to the sexual exploitation of children, including correspondence and communications with minors;
- (h) Child pornography or visual depictions of minors engaged in sexually explicit conduct, in sexually suggestive poses or wearing sexually suggestive clothing;

- (i) Evidence indicating how and when the Facebook account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crimes under investigation and to the Facebook account owner;
- (j) Evidence indicating the Facebook account owner's state of mind as it relates to the crimes under investigation;
- (k) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

RAS
F. # 2021R00415

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN RE: WARRANT TO FACEBOOK INC.

TO BE FILED UNDER SEAL

**Application for Non-Disclosure Order
Pursuant to 18 U.S.C. § 2705(b)**

No. 21-MJ-1208

**APPLICATION FOR ORDER COMMANDING FACEBOOK INC. NOT TO NOTIFY
ANY PERSON OF THE EXISTENCE OF WARRANT**

The United States requests that the Court order FACEBOOK INC. not to notify any person (including the subscribers and customers of the account listed in the warrant) of the existence of the warrant attached to the proposed Order submitted herewith for the period of one year from the date of the Order.

FACEBOOK INC. is a provider of an electronic communication service, as defined in 18 U.S.C. § 2510(15), and/or a remote computing service, as defined in 18 U.S.C. § 2711(2). Pursuant to 18 U.S.C. § 2703, the United States obtained the attached warrant, which requires FACEBOOK INC. to disclose certain records and information to the United States. This Court has authority under 18 U.S.C. § 2705(b) to issue “an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order.” *Id.*

In this case, such an order would be appropriate because the attached warrant relates to an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation, and there is reason to believe that its disclosure will alert the the targets to

the ongoing investigation. Specifically, the account listed in the warrant is believed to belong to an individual who is a target of the investigation, who is at large and who does not yet know of the investigation. Accordingly, there is reason to believe that notification of the existence of the attached warrant will seriously jeopardize the investigation, including by giving targets an opportunity to flee from prosecution, destroy or tamper with evidence, change patterns of behavior or intimidate potential witnesses. See 18 U.S.C. § 2705(b). Some of the evidence in this investigation is stored electronically and can be completely and permanently erased. Some of the evidence in this investigation involves communications that can be transferred to alternate platforms (including encrypted platforms and platforms beyond the jurisdictional reach of U.S. legal process). If alerted to the existence of the warrant, there is reason to believe that the targets under investigation will destroy that evidence and change their patterns of behavior.

WHEREFORE, the United States respectfully requests that the Court grant the proposed Order directing FACEBOOK INC. not to disclose the existence or content of the warrant attached to the proposed Order for the period of one year from the date of the Order, except that FACEBOOK INC. may disclose the warrant to an attorney for FACEBOOK INC. for the purpose of receiving legal advice.

The United States further requests that the Court order that this application and any resulting order be sealed until further order of the Court. As explained above, these documents discuss an ongoing criminal investigation that is neither public nor known to all of

the the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Dated: Brooklyn, New York

October 25, 2021

BREON PEACE
United States Attorney
Eastern District of New York

By: Rachel Shanies
Rachel A. Shanies
Assistant U.S. Attorney
(718) 254-6140

RAS
F. # 2021R00415

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN RE: WARRANT TO FACEBOOK INC.

TO BE FILED UNDER SEAL

No. 21-MJ-1208

ORDER

The United States has submitted an application pursuant to 18 U.S.C. § 2705(b), requesting that the Court issue an Order commanding FACEBOOK INC., an electronic communication service provider and/or a remote computing service, not to notify any person (including the subscribers and customers of the account listed in the warrant) of the existence of the attached warrant for the period of one year from the date of this Order.

The Court determines that there is reason to believe that notification of the existence of the attached will seriously jeopardize the investigation or unduly delay a trial, including by giving targets an opportunity to flee from prosecution, destroy or tamper with evidence, change patterns of behavior or intimidate potential witnesses. See 18 U.S.C. § 2705(b).

IT IS THEREFORE ORDERED under 18 U.S.C. § 2705(b) that FACEBOOK INC. shall not disclose the existence of the attached warrant, or this Order of the Court, to the listed subscriber or to any other person for the period of one year from the date of this Order, except that may disclose the attached warrant to an attorney for FACEBOOK INC. for the purpose of receiving legal advice.

IT IS FURTHER ORDERED that the application and this Order are sealed until
otherwise ordered by the Court.

Dated: Brooklyn, New York
October ²⁵ __, 2021

Cheryl Pollak

HONORABLE CHERYL L. POLLAK
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK